UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE
SOUTHERN DIVISION

DANA JONES, individually as parent and guardian of A.J., a minor, and on behalf of all others similarly situated, Plaintiff, v. SPECIALTY NETWORKS LLC, Defendant.	Case No._____ **CLASS ACTION COMPLAINT** JURY TRIAL DEMAND

Plaintiff Dana Jones ("Plaintiff"), individually and as parent and guardian of her minor daughter A.J., and on behalf of classes of similarly situated individuals (defined below), brings this action against Defendant Specialty Networks LLC ("Specialty" or "Defendant"). Plaintiff makes the following allegations based upon personal knowledge as to her own actions and upon information and belief as to all other matters, and she believes that reasonable discovery will provide additional evidentiary support for the allegations herein.

I. NATURE OF THE CASE

1. Specialty provides radiology information systems, digital transcription services, and Enterprise Practice Management solutions for medical facilities. Indeed, Specialty purports to "specialize" in support and storage for medical imaging technology.[1]

2. Specialty's partners' patients entrust Specialty's partners with their personally identifiable information ("PII") and protected health information ("PHI"), which Specialty's partners then use to obtain Specialty's services.

[1] *See* https://specialtynetworks.com/about-us/.

3. Specialty allowed that PII and PHI to be accessed by third parties. More troublingly, Specialty was aware as early as December 18, 2023—over eight months ago—that its systems had been compromised by an unauthorized third party. Yet it waited months to notify patients that their data had been compromised.

4. On or about August 15, 2024, Specialty finally admitted that an unauthorized individual accessed its systems on December 11, 2023 and acquired data stored within its systems (the "Data Breach"). Specialty has not disclosed how many individuals' PII and PHI—including personal, medical, and health insurance information, as well as Social Security numbers—was compromised in the Data Breach.

5. Plaintiff now seeks compensation under principles of common law negligence and unjust enrichment, as well as for breach of the Tennessee Consumer Protection Act ("TCPA"), for her damages and those of fellow Class members. Plaintiff also seeks injunctive relief to ensure that Specialty cannot continue to put patients at risk.

II. JURISDICTION AND VENUE

6. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 Class members, and one or more members of the classes are residents of a different state than the Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

7. This Court has personal jurisdiction over Defendant because it is headquartered in this District.

8. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), as Defendant resides, transacts business, committed an illegal or tortious act, has an agent, and/or can be found in this District.

III. PARTIES

9. Plaintiff Dana Jones is a resident of Chattanooga, Tennessee. On or about August 19, 2024, Plaintiff Jones received a letter from Specialty informing her that her PII and PHI had been compromised in the Data Breach.

10. Plaintiff Dana Jones is the parent and guardian of her minor daughter A.J., who is a resident of Chattanooga, Tennessee. On or about August 19, 2024, Plaintiff Jones received a letter from Specialty informing her that her daughter's PII and PHI had been compromised in the Data Breach.

11. Defendant Specialty Networks is a Tennessee limited liability company headquartered in this District at 1604 Gunbarrel Road, Chattanooga, TN 37421-3125. According to its filings with the Tennessee Secretary of State, Specialty has one member. On information and belief, Defendant's sole member is a resident of Tennessee. Defendant collects and maintains the PII and PHI of thousands of U.S. consumers.

12. Defendant's unlawful conduct was authorized, ordered, or performed by its directors, officers, managers, agents, employees, or representatives in the course of their employment and while actively engaged in the management of Defendant's affairs.

IV. FACTUAL ALLEGATIONS

A. The Data Breach

13. As outlined above, Specialty admitted it was the subject of a data breach that affected patients around the country. On December 11, 2023, unauthorized third-party

cybercriminals infiltrated the network that Specialty uses to store sensitive PII and PHI (including PII and PHI) of medical patients. These cybercriminals went undetected as they acquired highly-sensitive PII and PHI of thousands of patients.

14. The customer PII and PHI the hackers accessed names, dates of birth, driver's license numbers, Social Security numbers, medical record numbers, treatment and condition information, diagnoses, medications, and health insurance information.

15. Specialty inexplicably waited until August 2024, however, to begin notifying patients that their PII and PHI was compromised in the Data Breach. In fact, some customers were unaware for over eight months that their PII and PHI had been compromised.

16. Specialty had obligations to Plaintiff and to Class members to safeguard their PII and PHI and to protect it from unauthorized access and disclosure. Indeed, Plaintiff and Class members provided their PII and PHI to entities that provided it to Specialty with the reasonable expectation and mutual understanding that Specialty would comply with its obligations to keep such information confidential and secure from unauthorized access. Specialty's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies before the Data Breach.

17. As a result of the Data Breach, numerous data security experts are suggesting that affected consumers take steps to protect their identities.

B. Plaintiff Expected Specialty to Keep Her Information Secure.

18. Plaintiff Dana Jones provided her PII and PHI, as well as the PII and PHI of her minor daughter, to her healthcare providers as a condition of receiving products and services from those healthcare providers. Those providers then provided that PII and PHI to Defendant, which Defendant then stored and maintained.

19. Ms. Jones places significant value on the security of her PII and PHI, as well as the security of her minor daughter's PII and PHI, especially when receiving health services or health insurance services. She entrusted her sensitive PII and PHI to Specialty with the understanding that Specialty would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

20. Additionally, Plaintiff is very careful about sharing her PII and PHI. She has never knowingly transmitted unencrypted PII or PHI over the internet or any other unsecured source.

21. As a result of Specialty's exposure of Ms. Jones's and her daughter's PII and PHI, she will have to spend hours attempting to mitigate the affects of the Data Breach, including monitoring financial and other important accounts for fraudulent activity.

22. Given the highly-sensitive nature of the information that was compromised, Ms. Jones has already suffered injury and remains at a substantial and imminent risk of future harm. In addition, Ms. Jones has a continuing interest in ensuring that her and her daughter's PII and PHI, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

C. FTC Security Guidelines Concerning PII

23. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

24. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

25. In 2016, the FTC provided updated security guidelines in a publication titled *Protecting PII and PHI: A Guide for Business*. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention to the security of web applications—the software used to inform visitors to a company's website and to retrieve information from the visitors.

26. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

27. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

28. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their PII and PHI, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition

to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.[2]

29. Specialty was aware or should have been aware of its obligations to protect its customers' PII, PHI, and privacy before and during the Data Breach, yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, Specialty violated its obligations under Section 5 of the FTC Act.

D. Specialty Was on Notice of Data Threats and the Inadequacy of Its Data Security.

30. Specialty was on notice that companies maintaining large amounts of PII and PHI during their regular course of business are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information, such as the type of data at issue in this case.

31. At all relevant times, Specialty knew, or should have known, that the PII and PHI that it collected was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on similar companies, Specialty failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII and PHI from cyber-attacks that Specialty should have anticipated and guarded against.

32. It is well known among companies that store PII and PHI that sensitive information—such as the Social Security numbers and health information accessed in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[3]

---

[2] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement.

[3] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last visited Feb. 16, 2023).

33. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[4]

34. In light of recent high profile data breaches, including Microsoft (250 million records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Specialty knew or should have known that its electronic records would be targeted by cybercriminals.

35. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

E. The Data Breach Harmed Plaintiff and Class Members

36. Plaintiff and Class members have suffered and will continue to suffer harm because of the Data Breach.

37. Plaintiff and Class members face an imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and

[4] The HIPAA Journal, *Editorial: Why Do Criminals Target Medical Records* (Oct. 14, 2022), https://www.hipaajournal.com/why-do-criminals-target-medical-records.

PHI—thereby risking prosecution by listing it for sale on the dark web—if the PII and PHI was not valuable to malicious actors.

38. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

39. Malicious actors use PII and PHI to gain access to Class members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including PII and PHI of family, friends, and colleagues.

40. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

41. PII and PHI, like that stolen from Specialty, is "often processed and packaged with other illegally obtained data to create full record sets (fullz) that contain extensive information on individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[5]

[5] *See See* Maria Henriquez*, Iowa City Hospital Suffers Phishing Attack, Security Magazine* (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

42. Cybercriminals also maintain encrypted information on individuals to sell in "fullz" records because that information can be foreseeably decrypted in the future.

43. Specialty was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[6]

44. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[7]

As implied by the above AMA quote, stolen PII and PHI can be used to interrupt important medical services. This is an imminent and certainly impending risk for Plaintiff and Class Members.

45. The U.S. Department of Health and Human Services and the Office of Consumer Rights urges the use of encryption of data containing sensitive PII and PHI. As far back as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive PII and PHI. In announcing the fines, Susan McAndrew,

---

[6] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idINKBN0GK24U20140820.

[7] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED.ASS'N (Oct 4, 2019), https://www.ama-assn.org/practice-anagement/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

formerly OCR's deputy director of health information privacy, stated that "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[8]

46. As a HIPAA-covered entity, Specialty should have known about its data security vulnerabilities and implemented enhanced and adequate protection, particularly given the nature of the PII and PHI stored in its unprotected files.

47. Specialty issued misleading public statements about the Data Breach, including its data breach notification letters,[9] in which it attempts to downplay the seriousness of the Data Breach by stating that "we are not aware of the misuse of any affected individual's information."

48. Specialty's intentionally misleading public statements ignore the serious harm its security flaws caused to the Class. Worse, those statements could convince Class members that they do not need to take steps to protect themselves.

49. The data security community agrees that the PII and PHI compromised in the Data Breach greatly increases Class members' risk of identity theft and fraud.

50. As Justin Fier, senior vice president for AI security company Darktrace, observed following a recent data breach at T-Mobile, "[t]here are dozens of ways that the information that was stolen could be weaponized." He added that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates.[10]

---

[8] Susan D. Hall, *OCR levies $2 million in HIPAA fines for stolen laptops*, Fierce Healthcare (Apr. 23, 2014), https://www.fiercehealthcare.com/it/ocr-levies-2-million-hipaa-fines-for-stolen-laptops.

[9] An exemplar of which is available at https://static1.squarespace.com/static/65fb38019198445d318ea5c9/t/66be57719976ff0774626452/1723750257355/2024-08-14+-+Specialty+Networks+-+Substitute.pdf

[10] https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-un-carrier-un-safe/.

51. Criminals can use the PII and PHI that Specialty lost to target Class members for imposter scams, a type of fraud initiated by a person who pretends to be someone the victim can trust in order to steal sensitive data or money.[11]

52. Criminals can also use the PII and PHI that Specialty lost to commit medical identity theft.[12] These third parties can use an individual's name, Social Security number, health insurance information, or some combination thereof to see a doctor, get prescriptions, fraudulently submit claims to an individual's insurance provider, or get medical care—which could impact Plaintiff's or Class members' ability to access their own medical care or health insurance benefits, not to mention their credit.

53. The PII and PHI accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again.

54. Malicious actors can use Class members' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

55. As established above, the PII and PHI accessed in the Data Breach is also very valuable to Specialty. Specialty collects, retains, and uses this information to increase profits by providing services to health care providers. The patients whose PII and PHI Specialty collected and maintained value the privacy of this information and expect Specialty to allocate enough resources to ensure it is adequately protected.

56. Indeed, "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and

11 *See* https://consumer.ftc.gov/features/imposter-scams.
12 *See* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.

regulatory frameworks."[13] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[14] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

57. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

58. The PII and PHI accessed in the Data Breach is also very valuable to Plaintiff and Class members. Consumers often exchange PII and PHI for goods and services. For example, consumers often exchange their PII and PHI for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class members' PII and PHI has been compromised and lost significant value.

59. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is

[13] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, https://doi.org/10.1787/5k486qtxldmq-en.

[14] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[15]

60. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII and PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

61. Plaintiff and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the PII and PHI obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen PII and PHI, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and PHI and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiff and Class members will therefore need to continuously monitor their accounts for years to ensure their PII and PHI obtained in the Data Breach is not used to harm them.

62. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

63. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims experienced

[15] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

64. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."

65. Plaintiff and Class member customers have failed to receive the value of the Specialty services for which they paid and/or would have paid less had they known that Specialty was failing to use reasonable security measures to secure their data.

F. Defendant Failed to Take Reasonable Steps to Protect PII and PHI

66. Specialty requires its customers to provide a significant amount of highly personal and confidential PII and PHI to purchase its good and services. Specialty collects, stores, and uses this data to maximize profits while failing to encrypt or protect it properly.

67. Specialty has legal duties to protect patients PII and PHI by implementing reasonable security features. This duty is further defined by federal and state guidelines and laws, including HIPAA, as well as industry norms.

68. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiff's and Class members' PII and PHI was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiff and Class members were harmed. Plaintiff and Class members did not consent to having their PII and PHI disclosed to any third-party, much less a malicious hacker who could exfiltrate it and then sell it to criminals on the dark web.

69. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII and PHI of Plaintiff and Class members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time or for whom there was no reasonably anticipated future use.

70. Defendant's negligence in safeguarding the PII and PHI of Plaintiff and Class members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

71. Experts have identified several best practices that business like Specialty should implement at a minimum, including, but not limited to: educating all employees; requiring strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

72. Other best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

73. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

74. The foregoing frameworks are existing and applicable industry standards, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

75. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards, as evidenced by the Data Breach and the unreasonable length of time between the unauthorized access to Specialty's systems and Specialty's discovery of that unauthorized access.

76. The Data Breach was a reasonably foreseeable consequence of Defendant's inadequate security systems. Specialty certainly has the resources to implement reasonable security systems to prevent or limit damage from data breaches. Even so, Specialty failed to properly invest in its data security. Had Specialty implemented reasonable data security systems and procedures (*i.e.*, followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from infiltrating its systems and accessing its customers' PII and PHI.

77. Specialty's failure to implement reasonable security systems has caused Plaintiff and Class members to suffer and continue to suffer harm that adversely impact Plaintiff and Class members economically, emotionally, and/or socially. As discussed above, Plaintiff and Class members now face a substantial, imminent, and ongoing threat of identity theft, scams, and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores and diligently sift out phishing communications to limit potential adverse effects of the Data Breach, regardless of whether any Class member ultimately falls victim to identity theft.

78. In sum, Plaintiff and Class members were injured as follows: (i) theft of their PII and PHI and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII and PHI; (iii) the lost value of unauthorized access to their PII and PHI; (iv) diminution in value of their PII and PHI; (v) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (vi) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (vii) overpayments to Specialty for goods and services purchased, as Plaintiff and Class members reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII and PHI, which was not the case; and/or (viii) nominal damages.

79. Even though Specialty has decided to offer free credit monitoring for one year to its affected customers, this is insufficient to protect Plaintiff and Class members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiff and the Classes significant time and effort.

80. Plaintiff and Class members therefore have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages) that protects them from these long-term threats. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

V. CLASS ALLEGATIONS

81. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Federal Rule of Civil Procedure 23 as representative of the Classes defined as follows: All U.S. residents whose data was accessed in the Data Breach.

82. Specifically excluded from the Classes are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Classes are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

83. Class Identity: The members of the Classes are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact Class members.

84. Numerosity: The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, Class consists of thousands of individuals whose data was compromised in the Data Breach.

85. Typicality: Plaintiff's claims are typical of the claims of the members of the classes because all Class members had their PII and PHI accessed in the Data Breach and were harmed as a result.

86. Adequacy: Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has no interest antagonistic to those of the classes and is aligned with Class members' interests because Plaintiff was subject to the same Data Breach as Class members and faces similar threats due to the Data Breach as Class members. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes.

87. Commonality and Predominance: There are questions of law and fact common to the classes. These common questions predominate over any questions affecting only individual Class members. The common questions of law and fact include, without limitation:

a. Whether Defendant owed Plaintiff and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII and PHI;

b. Whether Defendant received a benefit without proper restitution, making it unjust for Defendant to retain the benefit without commensurate compensation;

c. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class members' PII and PHI;

d. Whether Defendant breached its duty to implement reasonable security systems to protect Plaintiff's and Class members' PII and PHI;

e. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiff and Class members;

f. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

g. When Defendant learned of the Data Breach and whether its response was adequate;

h. Whether Plaintiff and other Class members are entitled to credit monitoring and other injunctive relief;

i. Whether Defendant provided timely notice of the Data Breach to Plaintiff and Class members; and,

j. Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

88. Defendant has engaged in a common course of conduct, and Class members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customers' PII and PHI, as well as Defendant's failure to timely alert affected customers to the Data Breach.

89. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences.

Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under Federal Rule of Civil Procedure 23.

VI. CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

90. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

91. Defendant owed Plaintiff and Class members a duty to exercise reasonable care in protecting their PII and PHI from unauthorized disclosure or access. Defendant breached its duty of care by failing to implement reasonable security procedures and practices to protect this PII and PHI. Among other things, Defendant failed to: (i) implement security systems and practices

consistent with federal and state laws and guidelines; (ii) implement security systems and practices consistent with industry norms; (iii) timely detect the Data Breach; and (iv) timely disclose the Data Breach to impacted customers.

92. Defendant knew or should have known that Plaintiff's and Class members' PII and PHI was highly sought after by cyber criminals and that Plaintiff and Class members would suffer significant harm if their PII and PHI was compromised by hackers.

93. Defendant also knew or should have known that timely detection and disclosure of the Data Breach was required and necessary to allow Plaintiff and Class members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles and their health insurance carriers for fraudulent charges, contacting financial institutions, and cancelling or monitoring government-issued IDs such as passports and driver's licenses.

94. Defendant had a special relationship with Plaintiff and Class members who entrusted Defendant with several pieces of PII and PHI. Plaintiff and the Class were required to provide PII and PHI receiving health care services. Plaintiff and Class members were led to believe Defendant would take reasonable precautions to protect their PII and PHI and would timely inform them if their PII and PHI was compromised, which Defendant failed to do.

95. The harm that Plaintiff and Class members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to enact reasonable security procedures and practices, and Plaintiff and Class members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII and PHI accessed in the Data Breach is precisely the type of information that cyber criminals seek and use to commit cyber crimes.

96. But-for Defendant's breach of its duty of care, the Data Breach would not have occurred and Plaintiff's and Class members' PII and PHI would not have been accessed by an unauthorized and malicious party.

97. As a direct and proximate result of the Defendant's negligence, Plaintiff and Class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the compromised PII and PHI; illegal sale of the compromised PII and PHI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII and PHI; lost value of unauthorized access to their PII and PHI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

98. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

99. Specialty acquired and maintained the PII and PHI of Plaintiff and the Class that it received either directly or from its healthcare provider customers.

100. When Plaintiff and Class Members paid money and provided their PII and PHI to their doctors and/or healthcare providers, either directly or indirectly, in exchange for goods or

services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and pharmacies, including Specialty.

101. Plaintiff and Class Members entered into implied contracts with Specialty under which Specialty agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

102. Plaintiff and the Class were required to deliver their PII and PHI to Specialty as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

103. Specialty solicited, offered, and invited Plaintiff and Class Members to provide their PII and PHI as part of Specialty's regular business practices. Plaintiff and Class Members accepted Specialty's offers and provided their PII and PHI to Specialty, or, alternatively, provided Plaintiff's and Class Members' information to doctors or other healthcare professionals, who then provided to Specialty.

104. Specialty accepted possession of Plaintiff's and Class Members' PII and PHI for the purpose of providing services or Plaintiff and Class Members.

105. In accepting such information and payment for services, Specialty entered into an implied contract with Plaintiff and the other Class Members whereby Specialty became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII and PHI.

106. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Specialty and healthcare providers.

107. In delivering their PII and PHI to Specialty and paying for healthcare services, Plaintiff and Class Members intended and understood that Specialty would adequately safeguard the data as part of that service.

108. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

109. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII and PHI also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

110. Plaintiff and the Class Members would not have entrusted their PII and PHI to Specialty in the absence of such an implied contract.

111. Had Specialty disclosed to Plaintiff and the Class (or their physicians) that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their PII and PHI to Specialty (or to their physicians to provide to Specialty).

112. Specialty recognized that Plaintiff's and Class Members' PII and PHI is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

113. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Specialty.

114. Specialty breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PII and PHI as described herein.

115. As a direct and proximate result of Specialty's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Breach of the Tennessee Consumer Protection Act of 1977
Tenn. Code § 47-18-101 *et seq.*
(On Behalf of Plaintiff and the Class)

116. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

117. Defendant violated Tenn. Code Ann. § 47-18-104 by engaging in deceptive acts or practices in the conduct of its business and the furnishing of its services in the State of Tennessee.

118. Defendant's deceptive practices include omitting, suppressing, and concealing the material fact that it did not have and did not reasonably ensure that it reasonably or adequately secured Plaintiff's and Class Members' PII and PHI.

119. Defendant engaged in acts of deception and false pretense in connection with its accepting, collecting, securing, and otherwise protecting patient PII and PHI and engaged in the following deceptive trade practices, including:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' PII and PHI;

b. Failing to comply with data security standards during the period of the Data Breach;

c. Failing to comply with regulations protecting the PII and PHI at issue during the period of the Data Breach;

d. Failing to adequately monitor, evaluate, and ensure the security of its network and systems;

e. Failing to recognize in a timely manner that Plaintiff's and other Class Members' PII and PHI had been compromised; and

f. Failing to timely and adequately disclose that Plaintiff's and Class Members' PII and PHI had been improperly acquired or accessed.

120. Plaintiff's and Class Members' PII and PHI would not have been compromised but for Defendant's wrongful and unfair breach of its duties.

121. Defendant's failure to take proper security measures to protect sensitive PII and PHI of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiff's and Class Members' PII and PHI.

122. Plaintiff and Class Members conferred a benefit on Defendant—payment for medical services—in reliance on Defendant's omissions and deceptive practices. Had Defendant disclosed in any form, whether verbally, in writing, or via electronic disclosure that it did not adequately secure patients' PII and PHI, Plaintiff and Class Members would not have sought or purchased services from Defendant.

123. As a direct and proximate result of Defendant's fraudulent acts and practices, Plaintiff and Class Members were injured and lost money or property, and monetary and nonmonetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein.

124. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Defendant's fraudulent business practices

or use of their PII and PHI; reasonable attorneys' fees and costs under Tenn. Code Ann. § 47-18-109; injunctive relief; and other appropriate equitable relief.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

125. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

126. Plaintiff and Class members have an interest, both equitable and legal, in the PII and PHI about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately accessed in the Data Breach.

127. Defendant was benefitted by the conferral upon it of the PII and PHI pertaining to Plaintiff and Class members and by its ability to retain, use, and profit from that information. Defendant understood that it was in fact so benefitted.

128. Defendant also understood and appreciated that the PII and PHI pertaining to Plaintiff and Class members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

129. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that PII and PHI would not have been transferred to and entrusted with Defendant.

130. Defendant continues to benefit and profit from its retention and use of the PII and PHI while its value to Plaintiff and Class members has been diminished.

131. Defendant also benefitted through its unjust conduct by selling its services for more than those services were worth to Plaintiff and Class members, who would not have purchased Specialty's products or services had they been aware that Defendant would fail to protect their PII and PHI.

132. Defendant also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class members' PII and PHI.

133. It is inequitable for Defendant to retain these benefits.

134. As a result of Defendant's wrongful conduct as alleged in this Complaint (including, among things, its knowing failure to employ adequate data security measures, its continued maintenance and use of the PII and PHI belonging to Plaintiff and Class members without having adequate data security measures, and its other conduct facilitating the theft of that PII and PHI), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class members.

135. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' PII and PHI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

136. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and Class members in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

137. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

138. Plaintiff and Class members have no adequate remedy at law for Defendant's unjust enrichment.

139. Defendant is therefore liable to Plaintiff and Class members for restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically: the value to Defendant of the PII and PHI that was compromised in the Data Breach; the profits Defendant is receiving from the use of that information; the amounts that Defendant overcharged Plaintiff and Class members for its products and use of its services; and the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class members' PII and PHI.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

(a) That the Court determine that Plaintiff's claims are suitable for class treatment and certify the proposed Classes pursuant to Fed. R. Civ. P. 23;

(b) That the Court appoint Plaintiff as representative of the Classes;

(c) That Plaintiff's counsel be appointed as counsel for the Classes;

(d) That the Court award compensatory, statutory, and punitive damages;

(e) In the alternative, that the Court award nominal damages as permitted by law;

(f) That the Court award injunctive or other equitable relief that directs Defendant to provide Plaintiff and the Classes with free identity theft protection and credit monitoring, and to implement reasonable security procedures and practices to protect customers' PII and PHI that conform to relevant federal and state guidelines and industry norms;

(g) That the Court award reasonable costs and expenses incurred in prosecuting this action, including attorneys' fees and expert fees; and

(i) Such other relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b), Plaintiff demands a trial by jury of all issues properly triable to a jury in this case.

Dated: August 26, 2024

Respectfully submitted,

/s/ Alexandra M. Honeycutt

Alexandra M. Honeycutt (TN Bar No. 039617)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Tel: (865) 247-0080
ahoneycutt@milberg.com

Kaleigh N. Boyd, WSBA #52684*
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600/Fax: (206) 682-2992
kboyd@tousley.com

** Application for Admission Forthcoming*

Attorneys for Plaintiff and the Proposed Class